General Services Administration
National Archives and Records Service Washington, DC 20408

Date : APR 11 1980

Reply to Attn of : N

Subject : Systematic review of cryptologic information

To : NC, NN, NL

1. The Department of Defense has issued the attached "Special Procedures for Use in Systematic Review of Cryptologic Information Pursuant to Section 3-403 of Executive Order 12065."

2. NARS staff members handling national security classified information should be especially alert to recognize cryptologic information. Paragraphs 2 and 3 of the attachment will be helpful in this regard.

3. Procedures for the review and declassification of classified cryptologic information are clearly stated in paragraph 4 of the attachment. In summary, NARS is not authorized to take any unilateral declassification action on any cryptologic information.

4. NARS general and specific restrictions will continue to be applied to such cryptologic information as is declassified by appropriate agency authority as in the past. The donor restrictions imposed on donated historical materials will be applied prior to release.

5. Questions should be referred to NND (523-3165).

James E. O'Neill

JAMES E. O'NEILL
Acting Archivist
of the United States

Attachment

OFFICE OF THE DEPUTY UNDER SECRETARY OF DEFENSE
WASHINGTON, D. C. 20301

DEC 27 1979

POLICY REVIEW

MEMORANDUM FOR Director
Information Security Oversight Office
General Services Administration

SUBJECT: Special Procedures for Use in Systematic Review of Cryptologic Information Pursuant to Section 3-403 of Executive Order 12065

Reference is made to my memorandum (I-8363/79) of 17 September 1979 and to the letter of October 25, 1979 from the Deputy Director of the Central Intelligence Agency (CIA), both regarding the above subject.

As a result of the cited CIA letter, a number of adjustments to the attachment to my 17 September 1979 memorandum have been made that are responsive to the concerns expressed by the CIA. Those adjustments are reflected in the attached revised "Special Procedures for Use in Systematic Review of Cryptologic Information Pursuant to Section 3-403 of Executive Order 12065" that is forwarded for your dissemination to all Government departments and agencies other than the Department of Defense and its Components. The CIA has concurred in the attachment. It is requested that your forwarding letter make clear that the present attachment supersedes the one previously sent to the several other departments and agencies.

Your cooperation and assistance in this matter are appreciated.

John E. Ritzert
Acting Director of Information Security

Attachment - 60 cys

bcc furnished w/att:
NSA, D4
CIA, Mr. White (ISS)

OFFICE OF THE UNDER SECRETARY OF DEFENSE
WASHINGTON, D.C. 20301

POLICY

January 1980

SPECIAL PROCEDURES FOR USE IN SYSTEMATIC REVIEW OF CRYPTOLOGIC INFORMATION PURSUANT TO SECTION 3-403 OF EXECUTIVE ORDER 12065

1. General guideline: cryptologic information uncovered in systematic review for declassification of 20/30 year old government records is not to be declassified by other than U.S. government cryptologic agencies. The information may concern or reveal the processes, techniques, operations, and scope of signals intelligence comprising communications intelligence, electronics intelligence, and telemetry intelligence, or it may concern the cryptosecurity and emission security components of communications security, including the communications portion of cover and deception plans.

2. Recognition of cryptologic information may not always be an easy task. There are several broad classes of cryptologic information, as follows:

a. Those that relate to communications security (COMSEC). In documentary form, they provide COMSEC guidance or information. Normally, COMSEC documents and materials are accountable under the "Communications Security Material Control System." Examples are: items bearing "TSEC" nomenclature ("TSEC" plus three letters), "Crypto Keying Material" for use in enciphering communications, Controlled COMSEC Items (CCI), and cryptographic keying devices.

b. Those that relate to signals intelligence (SIGINT). These appear as reports in various formats that bear security classification, sometimes followed by a five-letter codeword (World War II's ULTRA, for example) and often carry warning caveats such as "This document contains codeword material," "Utmost secrecy is necessary . . . ." Formats will appear, for example, as messages having addresses, "from" and "to" sections, and as summaries with SIGINT content with or without other kinds of intelligence and comment.

c. Research, development, test, and evaluation reports and information that relates to either COMSEC or SIGINT.

3. Commonly used words that may help in identification of these documents and materials are "cipher," "code," "codeword," "communications intelligence" or "COMINT," "communications security" or "COMSEC," "cryptanalysis," "crypto," "cryptography," "cryptosystem," "decipher," "decode," "decrypt," "direction finding," "electronic intelligence" or "ELINT," "electronic security," "encipher," "encode," "encrypt," "intercept," "key book," "signals intelligence" or "SIGINT," "signal security," and "TEMPEST."

4. Special procedures apply to the review and declassification of classified cryptologic information. The following shall be observed in the review of such information:

a. COMSEC Documents and Materials. If records or materials in this category are found in agency or department files that are not under COMSEC control, refer them to the senior COMSEC authority of the agency or department concerned or by appropriate channels to the following address:

Director, National Security Agency/
Chief, Central Security Service
ATTN: Policy Staff
Fort George G. Meade, MD 20755

b. SIGINT Information.

(1) If the SIGINT information is contained in a document or record originated by a U. S. government cryptologic organization and is in the files of a non-cryptologic agency or department, such material will not be declassified. The material may be destroyed unless the holding agency's approved records disposition schedule requires its retention. If the material must be retained, it must be referred to the originating organization for systematic review for declassification.

(2) If the SIGINT information has been incorporated by the receiving agency or department into documents it produces, referral of the SIGINT information to the originator is necessary prior to any declassification action.